Mr. John Mott-Smith
Director of Voting Systems
Office of the Secretary of State
1500 11th Street
Sacramento CA 95814

23 Jul 04

Subject: Addendum to Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19 for AccuVote Optical Scan (AV-OS) Precinct Counter, Version 1.94W and 1.96.4.

Executive Summary

State certification testing was conducted 19-22 July, 2004, at Diebold offices in Coppell, TX, to certify two versions of the AccuVote Optical Scan (AV-OS), versions 1.94W and 1.96.4, with the new GEMS 1.18.19. The AV-OS, version 1.94W, was previously certified in California under an earlier version of GEMS. This testing was to ensure continued compliance with California election code and rules under the new GEMS 1.18.19 and for the newer AV-OS Version 1.96.4.

This test configuration was limited to the precinct and absentee counting (single counter) applications. In this form, votes are tallied on each ballot scanner and uploaded to the consolidating GEMS from the individual memory cards used by each ballot counter. We also tested uploading the unofficial results by modem. This testing excludes central count operations which, with multiple networked ballot counters, transfer the individual ballot records to the GEMS directly and then GEMS performs the tally operation.

The testing for this version configuration showed compliance with the California Election Code but has broadly published security weaknesses similar to those reported earlier in reports [RABA] about the Diebold DREs. In spite of these weaknesses, the tested configuration provides better security and functional support than the currently certified version and is recommended for certification in replace of the current version, with suitable Technical Security Plan procedures compatible with those suggested earlier for the Touch Screen DREs. AV-OS operations should be limited to using report formatting support options 194 US for the Firmware 1.94W version and 195/196 US for the Firmware 1.96.4 version until other report formatting options are documented and reviewed. This recommendation only applies to AV-OS where the results are tallied on the unit and uploaded from the memory card.

References:

1. [RABA] *RABA, Trusted Agent Report Diebold AccuVote-TS Voting System,* 20 January, 2004

2. [SVF0624] Freeman, *Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19, Key Card Tool Rev 1.0.1 , Voter Card Encoders (VCE) Rev 1.3.2, and AccuVote Touch Screen DRE (AV-TS R6), Firmware 4.3.15D*, 24 Jun 2004

3. [GEMS-U] Diebold, *GEMS 1.18 User's Guide*, Rev 9.0, 13 Feb 2004

4. [CA OS Proc] Diebold, *California AccuVote OS Procedures*, Sep 2002

5. [1.94W-U] Diebold, *AccuVote-OS 1.94 Precinct Count User's Guide,* Rev 3.0 16 Aug 2003

6. [1.96.4-U] Diebold Document, *AccuVote-OS 1.96 Precinct Count User's Guide*, Rev 3.0 16 Aug 2003

Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following revisions:

a. Diebold's GEMS Version 1.18. 19.
b. Diebold's AV TS-R6, Version 4.3.15D
c. Key Card Tool, Revision 1.0.1
d. Voter Card Encoder, Revision 1.3.2
e. AV-OS, Firmware Version 1.94W (currently certified with GEMS 1.18.18)
f. AV-OS, Firmware Version 1.96.4 (new).

The AV-Optical Scan Ballot Counter (AV-OS) Firmware Version 1.94W is currently certified in California under GEMS 1.18.18. A recent certification test and report [SVF0624] on the revised GEMS 1.18.19 reviewed compliance with the AccuVote Touch Screen Revision 6 (AV-TS R6) using Ballot Station Version 4.3.15D. The revision incorporated significant security upgrades as well as fixed several minor problems identified from earlier releases. The new or revised functionality includes consolidation of the AVServer functions for AV-OS and AV-TS into a single function and necessitated retesting support of the earlier AV-OS 1.94W as well as testing the newer 1.96.4 version of AV-OS. The 1.96.4 version provides minor changes supporting more flexibility in handling of absentee ballots and changes expected to support compatibility with future updates.

In addition, errors noted in prior testing and reviewed in this retest are:

1. The Statement of Vote Counts (SOVC) did not correctly report the turn out data (corrected)
2. System errors noted with specific .abo files (specified safe files; see comments below).

NASED Qualifications

1. GEMS 1.18.19
   a. Ciber Report, dated 02-03-04 GEMS1.18.19 Final Report, A3a
   b. Ciber Report, dated 05-28-04 GEMS1.18.19 Final Report, A4a

2. AccuVote-OS
   a. Wyle Report, Oct 1996, Report No. 46098-01, (Original report)
   b. Wyle Report, Dec 1999, Report No. 46095-01, Change Release Report of the AccuVote-OS Ballot Counter Voting Machine (Firmware Change Release 1.94W).
   c. Wyle Report, dated 05/30/2003, Report No. 46058-05, Change Release Report of the AccuVote-OS Ballot Counter Voting Machine (Firmware Change Release 1.96.4).

3. Wyle Report, 06/04/2004, Report No. 48619-02, Change Release Report of the AccuVote-TS R6 DRE Voting Machine (Firmware Change Release 4.3.15D).

4. NASED Qualification: dated 5/20/04, N-1-06-12-12-002 (1990) includes:
   a. GEMS 1.18.19.
   b. AV-OS 1.94W.
   c. AV-OS 1.96.4.
   d. Others reported in [SVF0624].

Test Report Results

The test election was based on the San Diego 2002 Primary and General with the addition of Presidential race (with semi-fictional candidates to complete General election) in seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing DTS voter participation and reporting with the Republican DTS not permitting participation in Presidential nominations. For this test, a backup copy of the election used in the prior GEMS 1.18.19 test for the AV-TS R6 was loaded and reset to use the AV-OS ballot counters.

Security Access Controls

This release of GEMS 1.18.19 and AV-TS R6 provides substantially improved security to the AV-TS R6 ballot stations. The security issues were described in the previous report [SVF0624]. Except for those related only to GEMS, none of the security enhancements involved the AV-OS. For comparison, the following items repeat the earlier list but indicate the current application to AV-OS. The election procedures for the AV-TS and AV-OS are being rewritten to address some of these items but are not finished at in time to be included in this report.

The following security weaknesses were noted in testing:

Item	GEMS	TS	OS
1. Weak security of the basic server and operating system	Yes	n/a	n/a
2. GEMS database is accessible by DAO-supported programs	Yes	n/a	n/a
3. GEMS passwords are too weak	Yes	n/a	n/a
4. SSL/TLS encryption may be disabled	Yes	uses	n/a
5. Default encryption keys published (but may be changed)	Yes	uses	n/a
6. Default passwords/pins are hardcode	Yes	Yes	n/a
7. Some passwords/pins restricted to four digits.	Yes	Yes	Yes
8. Key locks on access panels are not secure		Yes	Yes
a. Memory card not secure		Yes	Sealable
b. Serial/Parallel ports not secure		Yes	Yes
9. PS/2 Keyboard port not secure		Yes	n/a
10. (new) Modem not secure		Unused	Yes

. Notes:

1. Encryption. Security experts are calling for encryption on the transfer media (memory cards, smart cards, and data lines) and internal data structures. Static and dynamic encryption are being added (SSL/TLS is part of that process) by Diebold to the DREs but are not implemented in the AV-OS version. In the precinct level and untested central count method, this encryption is recommended but may not be as critical in more limited central office absentee count where the counter and paper ballots are under active, direct supervision.
2. The modems on the AV-TS are not used in California but are internal (present) with exterior connections. In the AV-OS, the modems are used to upload unofficial results from precincts, but are not secure. Procedurally, the modem connection should have been used only for the unofficial reporting when polls closed and should be confirmed and monitored at both ends during such use. The official results are uploaded later using the actual memory card in a direct serial connection. Future versions should include encrypted, error reporting protocols, especially including secure verification of the sender, receiver, and message content.
3. A password field is available in GEMS to assign a new password for the AV-OS but the password (supervisor 'PIN') is restricted to one to four digits in the AV-OS.
4. The I/O ports in the back of the AV-OS unit are inaccessible when the unit is mounted on a ballot box but the locking mechanism to secure it suffers from the same weakness as the

AV-TS panel locks. However, the tamperproof seals for this lock may not be as effective since the locking mechanism may need to be opened clear jams and to get access to the power switch. At a minimum, a manual log may need to be kept to show when and why the back panel was accessed.

Other Known Problems

1. As mentioned in the prior report [SVF0624], options exist in the GEMS to select options that are not allowed or desirable under California procedures. I recommended that a reference be added to the California AV-TS procedures to provide a checklist for such options. For the AV-OS, a special case of a similar problem exists.

When setting up the AV-OS, the GEMS must be enabled to work with the AV-OS in a special window, AV-OS Options. AV-OS Options window in GEMS (see attachment) controls a number of optional settings for the election including

- selecting the firmware version to be used in the AV-OS;
- the selection and formats for reports to be printed on the log printer;
- setting up a remote network server (not approved);
- choices for how the counter responds to various problem type ballots; and
- controls the absentee ballots and straight-party (not approved) ballots will be interpreted and tallied.

During earlier testing with this equipment, problems were encountered with the choice of reporting formats. These involve the selection of special files, the .abo files that are installed with the GEMS software. Allegedly involving only minor formatting choices for the AV-OS internal printer reports, we have discovered that they also effect the supervisor menu options and may control some messages recorded on the log files.

Recommendations:

a. Diebold is to physically remove the obsolete or inappropriate .abo files from the California installation (this may be procedural). This is in addition to specifying which files may be used in the California AccuVote-OS Procedures.

b. Diebold is to catalog and report on what it is that each of the .abo files retained does.

c. Diebold is to provide the source code for the cataloged .abo files for review to confirm that the features described are complete, accurate, and do only what is defined.

d. Only the 194 US and 195/196 US files should be used until the other steps are completed and reviewed.

With adequate descriptions and verification, it may be unnecessary to actively test all the catalogued and recommended files for use although future state certification testing should include the use of non-ITA tested .abo files.

2. The modems were tested for operational problems with simple result uploads on local telephone lines (one internal and one external) while both are trying to access using a single telephone input line. In actual use, these will be using multiple lines, probably with roll-over circuits. Before elections, if these telephone modems are to be used, the telephone setup should be thoroughly tested with as many simultaneous inputs as possible (such as during the setup Logic and Accuracy testing) to confirm the connection will work and will respond correctly if a connection is dropped during transmission. For security reasons, the modems should not be uploaded until a verified backup of the database and setup is made and secured for use when the actual memory cards are brought forward for the official canvass processing.

Conclusion

The testing for this version configuration showed compliance with the California Election Code but has broadly published security weaknesses similar to those reported earlier in reports about the Diebold DREs. In spite of these weaknesses, the tested configuration provides better security and functional support than the currently certified version and is recommended for certification in replace of the current version, with suitable Technical Security Plan procedures compatible with those suggested in the June 2004 report on the AV-TS R6. AV-OS operations should be limited to using report formatting support options 194 US for the Firmware 1.94W version and 195/196 US for the Firmware 1.96.4 version until other report formatting options are documented and reviewed. This recommendation only applies to AV-OS where the results are tallied on the unit and uploaded from the memory card.

Sincerely,

Steven V. Freeman

Two Attachments:

A. Hardware Description with a list of the test configuration components.
B. Test Election Design

Attachment A.

Hardware Descriptions

AccuVote-OS Optical Scan Ballot Counter

The AccuVote-OS is a mark sense optical scan device principally designed to read and tabulate ballots at the polling place.

In this mode, it is mounted on a ballot box equipped with a diverter which can be used to deflect ballots into two of three bins in the standard ballot box. (The ballot box was not used in this test; it has been in long term use within California and no issues were known requiring its use in the test). The lock used to latch the counter to the ballot box is not considered secure and a tamperproof seal may need to be considered. However, the latch may need to be opened to clear jams and access the power switch so other procedures may need to be defined. The operation of unlocking the latch and pulling the counter away from the ballot box should be clearly visible to observers and poll officials. The AV-OS has also been used centrally to count absentee ballots and, in smaller counties, as a central counter in its own right. In the latter two uses, more than one AV-OS may be used. As a central counter, an optional configuration, also identified as "central count", networks more than one AV-OS to a central server running GEMS. In this configuration, only the ballot images are processed and the tally operation is performed by a unit in the GEMS software. This configuration was not tested at this time.

The firmware is installed as an EEPROM chip on the motherboard which is not intended to be accessed by the user (the use of tamperproof paper seals both on the installed chip and on the case for improved security). The election specific database with ballot definitions is installed in a memory card which is left resident in the AV-OS to record results. The memory card in installed in a slot on the front of the unit. A metal bar drops across the installed card and can be sealed with a tamperproof wire seal (first picture below). The memory card is programmed while installed in an AV-OS unit connected with a serial cable connected to the back panel (second picture below)

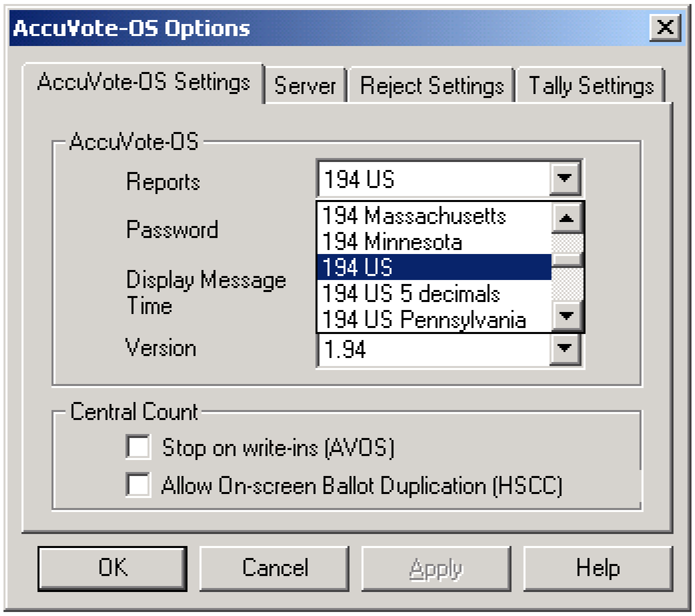
More than one unit can be connected for multiple downloads from the GEMS server using a serial port multiplexer (Diebold uses a DigiPort device). This setup is also used to upload results from memory cards using one or more units after polls closed and the cards are brought to a central location for uploading. Up to eight units may be connected using the DigiPort unit provided in the test. This setup is not used while counting ballots.

To upload, the memory card from the unit counting ballots must be installed in an AV-OS unit that has a serial connection to the reporting PC with GEMS installed and the results uploaded to the AVServer component of GEMS. The protocol of the electronic transfer has been proven to be vulnerable to interception; for uploading official results, the cable connection should be direct and restricted to short distances where the connection is under observation at all time. Vote totals are also stored independently in memory and can be recovered after the election as an independent record but again must be transferred via an AV-OS.

For unofficial results shortly after the polls close, larger counties may want to forward immediate, unofficial results via modem. An internal modem socket is accessible on the back panel and is not accessible while the device is latched into a ballot box. Such unofficial transmissions are inherently insecure (no security is provided on the upload protocol although some error detection is enabled). Full Summary and all precincts printed reports should be produced and secured before such a link is used. Before and during the dial-up connection, operators at both the AV-OS and GEMS server side should be in communications and confirm the connection is being made and the link is established and maintained through the upload (the GEMS operator monitors through the AVServer application in GEMS). We tested this setup to ensure simultaneous attempts to access a single modem on the GEMS server does not cause a conflict or result in drop of information and encountered no problems. If this is used in a real election, the connection is more likely to be through a roll-over setup for several lines. The full setup should be tested before actual use with as many simultaneous inputs to the same line as possible. A test upload of the Logic and Accuracy deck count is a good time to do this test with an actual review of the ballot counts in the Summary report to ensure counts were uploaded accurately. Official results should still be uploaded by a secure, physical transfer of the memory cards a central counting location.

The internal log printer, a thermal printer, is located under a key locked panel on the left side and is normally locked during precinct ballot counting. The printer cover lock is an insecure lock and may need to be protected while the polls are open with a tamperproof seal.

AV-OS Options:



AccuVote-OS

Reports: 194 US

- 194 Massachusetts
- 194 Minnesota
- 194 US
- 194 US 5 decimals
- 194 US Pennsylvania

Password

Display Message Time

Version: 1.94

Central Count

☐ Stop on write-ins (AVOS)

☐ Allow On-screen Ballot Duplication (HSCC)

The AV-OS requires a special configuration to be setup in GEMS for election programming. The screen above shows the AccuVote-OS Options screen with the basic settings. In this screen, the firmware version (Version has 1.94 selected) and the Reports (a pull down showing some of the report options with 194 US highlighted.)

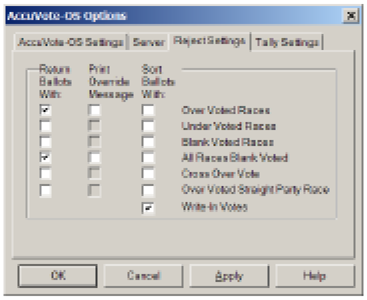
The Reports format is a selection between special files, installed in GEMS as .abo files. Reports selected must match the firmware version (Firmware 1.94W must use reports labeled as ‘194 xxxx’). No documentation has been provided at this time describing what the different Report options provide. Federal ITA testing has only verified 194 US for the 1.94W firmware and 195/196 US for the 1.96.4 firmware. Earlier state certification testing found serious errors with other Reports options and revealed that the .abo files effect the Supervisor menu options presented, report formats, and are suspected to effect log reporting. The 194 US format automatically generates a Summary and all Precinct report when polls are closed. Some California counties wish to use an alternate format such as 194 US Summary which automatically prints the Summary but permits the operator to choose whether any or all of the precincts will be printed at that time. The full Summary and all Precincts report takes a long time to complete and is unavoidable when the power is turned off and turned back on. During this test, we used the 194 US Summary report and did not encounter any problems. However, since no descriptions are available to determine what other changes may be involved, it is not clear that the test was adequate to recommend use. Diebold has been asked to provide a catalog description of what the differences are between the various reports that may potentially be used in California and copies of the .abo source files to verify that descriptions are complete. Pending a review of that information, other .abo report formats may be recommended or identified as candidates for further testing. Report format files not appropriate for California use should be disabled and/or removed from the installed versions as the consequences of using an improper version may be significant.

A password field is also provided to change the supervisor password. The AV-OS only has Yes and No buttons so any password other than 0’s or 1’s is cumbersome (the button must be go through a Yes/No selection to get more than a ‘0’). The Password field will actually accept a one digit password but the AV-OS requires four digits; a ‘1’ password must be entered at the AV-OS unit as ‘0001’. The other options in this tab were not part of the test configuration and were not tested. [redacted]

[redacted]

For the password to be an effective deterrent, passwords other than '0000', '0001', '1000' should be used; preferably, the password should include digits other than '0' and '1' and be more than a one digit password ('000x').

The Server tab is for uploading to an intermediate server connected and was not tested at this time due to security concerns with that configuration. The Server options should not be used at this time pending further security improvements.



Return Ballots With:	Print Override Message	Sort Ballots With:	
☑	□	□	Over Voted Races
□	□	□	Under Voted Races
□	□	□	Blank Voted Races
☑	□	□	All Races Blank Voted
□	□	□	Cross Over Vote
□	□	□	Over Voted Straight Party Race
		☑	Write-In Votes

The Reject Settings controls whether a ballot will be returned to a voter for reconsideration. Over Voted Races and All Races Blank Voted (Blank ballots) are recommended for precinct counting but may be turned off when used for absentee ballot counting in favor of Sort Ballots where the ballot is delivered to the second ballot bin for manual review. However, the same setting must be used for all AV-OS, whether used as precinct or absentee counting, used in the same election. The Print Override Message, when selected, prints a log item showing override actions; counties using the system have allegedly turned this option off because the sound of the printer has bothered them. However, this means that no log reports are being made of how much/frequently the ballots are being rejected for voter review.

The options set in the example figure are recommended as a minimum setting for precinct operations.

Test Configuration Inventory

1. Dell Power Edge 600SC, HH18021 Chassis S/N
   a. 1.8 gigahertz, Pentium 4 processor
   b. 1 MByte RAM
   c. 20 GByte IDE Internal Hard Drive
   d. PLEXTOR CD-R PX-W1210S SCSI CdRom Drive
   e. 3.5 Diskette Drive
   f. ARCHIVE Python 06408-XXX SCSI Sequential Tape Drive (not used)
   g. Digi AccelePort Xem-PCI bus card
2. DigiPorts 8/EM, PC/8em DB25, S/N: (S) V 21488435. Port 1 (COM3) and 2 (COM4)
3. Hewitt Packard Laser 1200 Printer.
4. Hayes Accura Modem External V.92 for PC-US, P/N: H08-163286, S/N 1-84-H08-15328-C1-0009 (test only)
   (Normal installed version is U.S. Robotics Sportster)
5. Commercial-Off-The-Shelf Software
   a. MS Windows 2000 Server, Service Pack 4 (Build 2195) w additional patches for SP5.
      i. Window Internet Explorer 6.00.2800.1106

b. Adobe Acrobat Version 6.0.0.2003051900
c. Nero CD/DVD Rom Burning Suite, Version 6,
d. WinZip 8.1, SR1

Note: All the above were installed using commercial installation sets on a clean system. Some additional packages were installed such as the Kodak picture utilities as included in the MS Windows 2000 install but are not germaine to this test

e. Crystal Reports. Loaded by the GEMS application as part of its install.

6. Five AccuVote-OS Optical Scan Ballot Counters
   a. Firmware Version 1.94W, factory installed as an EEPROM in each unit.
      i. M/N 79811-03 S/N 80599
      ii. M/N 79811-04 S/N 30874
   b. Firmware Version 1.96.4, factory/field installed as an EEPROM in each unit.
      i. M/N 79811-03 S/N 75708
      ii. M/N 79811-03 S/N 80599*
      iii. M/N 79811-03 S/N 87564
      iv. M/N 79811-04 S/N 30743
      v. M/N 79811-04 S/N 30874*

Notes:

1. Three units became disabled for reasons not germane to the test and were replaced to complete testing with the 1.94W units upgraded to 1.96.4. One of the 1.94W units originally had a problem with the 1.94W firmware chip but operated with no problems when the 1.96.4 chip was installed.
2. The units are manufactured in two different locations. UL Certification required manufacturing I.D.s with the location to be encoded in the M/N as the -03 and -04 designations. The -03 machines were manufactured in McKinney, TX, and the -04 machines in Lexington, NC.

7. Diebold Software
   a. GEMS 1.18.19.
      i. 194us.abo
      ii. 194ussm.abo
      iii. 195/196us.abo
      iv. (18 other .abo files not tested)
   b. KeyCardTool Application Version 1.0.1
   c. WINNT .dll files
      i.

Attachment B.

Test Election Design

	Precinct	1	2	2	3	4	5	6	7	8	9	10
Type	**Split**		1	2								
SW	Federal, STATE	x	x	x	x	x	x	x	x	x	x	x
SD	Board of Equal 3	x	x	x	x	x	x	x	x	x	x	x
SD	CONGRESS 49	x	x	x								
SD	CONGRESS 50				x	x						
SD	CONGRESS 51						x	x				
SD	CONGRESS 52								x	x		
SD	CONGRESS 53										x	x
SD	STATE SENATE 36	x	x									
SD	STATE SENATE 37				x		x					
SD	STATE SENATE 38			x		x						
SD	STATE SENATE 39								x		x	
SD	STATE SENATE 40							x		x		x
SD	ASSEMBLY 66	x							x			
SD	ASSEMBLY 74				x					x		
SD	ASSEMBLY 75		x	x							x	
SD	ASSEMBLY 76						x	x				
SD	ASSEMBLY 77					x						x
U	COUNTY, Unincorporated		x					x				
C	CHULA VISTA			x								
C	LEMON GROVE	x										
R	PORTER VISTA					x						
S	Measure	x	x	x	x	x	x	x	x	x	x	x

C city, M Military, R unincorporated remainder of county, U Unincorporated place in a county.

Further details on test election makeup and

The test election was modified from the San Diego by combining various districts and races into a selection of ten precincts which concisely included samples of state, statewide district (State Senate and Assembly Districts), judicial, (See Test Design Matrix above). Only first five precincts with one split precinct were used in this test due to testing time limits but these are adequate to test all but the supervisor district rotations.

Testing was completed using a pre-marked Logic and Accuracy deck. The test deck was used to verify basic election definition and verify the rotation was set up correctly on the 1.94W units. An error had been made in the test deck definition (the error was in the test setup and not GEMS), but, since the ballots were already printed, the test continued with the revised rotation.

Additional ballots were marked to test response to common voter errors and some ballot tampering changes.

A total of 1103 primary ballots were cast. exercising the following ballot logic and conditions:

1. Primary party ballots with DTS voting and reporting
2. Non-Partisan races
3. Split precinct
4. Vote for 2 of 5,
5. Write-in votes (including potential over-vote conditions)
6. Blank ballots
7. Rotation based on assembly district at state, state districts, and local levels
8. (Multiple languages. Printed ballots were provided in English, Spanish, and Vietnamese)
9. Long names in candidate fields.
10. Turn-out statistics on final summary reports
11. Measures
12. Polls open, close, and report printing.
13. Review of audit logs.
14. Consolidating absentee and Election Day precinct voting.

The basic test was repeated using a 300 General Election deck for the same test objectives, less primary unique logic, plus

15. Power interruptions.
16. Simultaneous modem uploads competing for single input modem.

The basic scan unit for the AV-OS ballot counter has been in use in California for several years and no significant problems with the unit were reported to me from actual use.